G. Configure indexer discovery

H. Enable listeners on search peers

I. Create 3 indexes

J. Disable search pears UI

K. Install license

L. configure monitor console

K. intall linux and windows app from splunkweb in order to onboard windows and Linux data to splunk.

======================================================================================================================

Use indexer discovery to connect forwarders to peer nodes

https://docs.splunk.com/Documentation/Splunk/9.4.0/Indexer/indexerdiscovery

The manager node enables indexer discovery.

The manager and forwarders share a security key.

Forwarders will send data to peer nodes weighted by the total disk capacity of the peer nodes' disks.

The forwarders use indexer acknowledgment to ensure end-to-end fidelity of data.

##In the manager node's:server.conf:

[indexer\_discovery]

pass4SymmKey = splunk1234

indexerWeightByDiskCapacity = true

https://docs.splunk.com/Documentation/Splunk/9.4.0/Indexer/indexerdiscovery

On the DS create app in deployment-app folder

mkdir atlgsdach\_all\_indexers\_descovery\_base/local -p

In each forwarder's outputs.conf:

[indexer\_discovery:manager1]

pass4SymmKey = splunk1234

manager\_uri = https://172.31.1.193:8089

[tcpout:group1]

autoLBFrequency = 30

forceTimebasedAutoLB = true

indexerDiscovery = manager1

useACK=true

[tcpout]

defaultGroup = group1

## Enable listener on the indexers

On the Manager Node.

https://docs.splunk.com/Documentation/SplunkCloud/latest/Forwarding/Enableareceiver

mkdir atlgsdach\_all\_indexers\_base/local -p

cd /opt/splunk/etc/manager-apps/atlgsdach\_all\_indexers\_base/local

vi inputs.conf

[splunktcp://9997]

disabled = 0

./splunk apply cluster-bundle

./splunk apply cluster-bundle --skip-validation

===============================================

Create indexes

###create a new app in manager node and vi indexes.conf and deploy to indexers to store windows and linux logs

mkdir atlsdach\_all\_indexers\_base/local -p

cd /opt/splunk/etc/manager-apps/atlsdach\_all\_indexers\_base/local

vi indexes.conf

###base with 3 storage - hot is a fast drive, warm is a medium speed drive, and cold is a slow drive

[volume:one]

path = /opt/splunk/hot/one/

maxVolumeDataSizeMB = 40000

[volume:two]

path = /opt/splunk/warm/two/

maxVolumeDataSizeMB = 60000

[volume:three]

path = /opt/splunk/cold/three/

maxVolumeDataSizeMB = 80000

============================================================

[atlgsdach\_os\_prod]

homePath = volume:one/atlgsdach\_os\_prod/db

coldPath = volume:three/atlgsdach\_os\_prod/colddb

coldToFrozenDir = /opt/splunk/frozen/atlgsdach\_os\_prod/frozendb

thawedPath = /opt/splunk/thawed/atlgsdach\_os\_prod/thaweddb

maxHotSpanSecs = 2592000

frozenTimePeriodInSecs = 7776000

maxDataSize = auto

maxTotalDataSizeMB = 102400

repFactor = auto

======================================================

**[atlgsdach\_linux\_prod]**

**homePath = volume:one/atlgsdach\_linux\_prod/db**

**coldPath = volume:three/atlgsdach\_linux\_prod/colddb**

**coldToFrozenDir = /opt/splunk/frozen/atlgsdach\_linux\_prod/frozendb**

**thawedPath = /opt/splunk/thawed/atlgsdach\_linux\_prod/thaweddb**

**maxHotSpanSecs = 2592000**

**frozenTimePeriodInSecs = 7776000**

**maxDataSize = auto**

**maxTotalDataSizeMB = 102400**

**repFactor = auto**

=====================================================

[atlgsdach\_windows\_prod]

homePath = volume:one/atlgsdach\_windows\_prod/db

coldPath = volume:three/atlgsdach\_windows\_prod/colddb

coldToFrozenDir = /opt/splunk/frozen/atlgsdach\_windows\_prod/frozendb

thawedPath = /opt/splunk/thawed/atlgsdach\_windows\_prod/thaweddb

maxHotSpanSecs = 2592000

frozenTimePeriodInSecs = 7776000

maxDataSize = auto

maxTotalDataSizeMB = 102400

repFactor = auto

=====================================================

/opt/splunk/etc/system/local

web.conf.

[settings]

startwebserver = false

./splunk reload deploy-server –class <my serverclass\_name>

./splunk apply cluster-bundle

./splunk apply cluster-bundle --skip-validation

./splunk set deploy-poll https://172.31.1.241:8089

Create the below apps on ds and push them to the forwarders

all\_base\_inputs\_linux all\_base\_inputs\_windows